What Is Claimed Is:

1. A method for optimizing the operation of an anti-virus computer program for use with an operating system, comprising the steps of:

detecting a request for closure of an opened computer file;

determining in response to a closure request if the opened computer file has been modified since being opened;

scanning said opened file for viruses before closure only if said opened file has been modified; and

closing said file if unmodified, and closing said file after scanning for viruses if found virus free.

2. The method of Claim 1, further including before said detecting step, the steps of:

determining whether said operating system includes a "dirty cache buffer" to raise or set a modification flag relative to a file being modified during the time it has been open, a computer code being indicative of said flag; and

using the computer code for a raised or set modification flag, if available, for carrying out said modification determining step by checking for the presence of a raised modification for said file.

3. The method of Claim 2, wherein if it is determined that said operating system does not provide a file modification flag, said method further includes the steps of:

establishing a "dirty cache buffer";

and

raising a modification flag in said "dirty cache buffer" if an opened file associated with said flag has been modified by a write operation.

A2

4. The method of Claim 1, wherein said operating system includes a "dirty cache buffer" for providing a computer code for a modification flag indicative of the modification of an open file, said method further including in said modification determining step, the step of:

detecting the presence of said modification flag to determine if the associated opened file has been modified.

5. The method of claim 4, further including the steps of:

scanning a file for viruses in response to a request for opening the file;

opening said file if virus free;

establishing a cache buffer memory for storing upon opening of a file only a virus vulnerable portion of that file that a virus must use to enter and infect said file;

said modification determining step including the steps of:

indicating an open file is unmodified in the absence of an associated modification flag;

responding to the presence of a modification flag by comparing a portion of said open file to the associated unmodified virus vulnerable portion of said file in said cache buffer memory to determine if the portion of the open file has been modified since the opening of the file;

indicating the opened file is unmodified is the virus vulnerable portion is unmodified; and

indicating the opened file is modified if the virus vulnerable portion is modified.

6. The method of Claim 1, wherein said step of determining in response to a closing request if the opened computer file has been modified since being opened includes the step of:

monitoring network protocols to determining if a write packet was initiated for a given open file.

7. A method for optimizing operation of an anti-virus program in an operating system, said operating system including programming for raising a flag indicative of modification of an open file during the time the file has been open, said method including the steps of:

detecting the event of a request for closing said file being made to said operating system;

determining whether said modification flag has been raised by said operating

system for said open file;

scanning said open file, in response to said modification flag, for viruses before permitting said operating system to close said file; and

skipping said step of scanning for viruses before closure of said open file, whenever said modification flag is not present.

A2

8. A method for optimizing the operation of an anti-virus program in use in an operating system, said operating system including programming for raising a flag indicative of modification of an open file during the time the file has been open, said method including the steps of:

scanning a file for viruses in response to a request from an associated computer user to open and gain access to said file;

permitting said file to be opened if virus free;

storing upon opening a virus vulnerable unmodified portion of said open file;

detecting the event of a request for closing said open file being made to said operating system;

determining whether said modification flag has been raised by said operating system for said open file;

scanning said open file, in response to said modification flag, for viruses before permitting said operating system to close said file; and

skipping said step of scanning for viruses before closure of said open file, whenever said modification flag is not present;

responding to the presence of a modification flag by comparing the stored unmodified virus vulnerable portion of said file to the associated portion of said open file to determine if that portion has been modified during the time the file has been open; and

skipping said step of scanning for viruses before closure of said open file if the virus vulnerable portion of said open file is unmodified.

A2

9. A computer program product for detecting computer viruses on a file server, the file server providing file storage and retrieval services for at least one client computer over a network, said computer program product comprising:

computer code for detecting an open request from a client computer, the open request asking for a requested file from the file server;

computer code for scanning said requested file for computer viruses, whereby the file server is permitted to provide said requested file to the client computer if no computer viruses are found therein;

computer code for detecting a close request from the client computer associated with said requested file;

computer code for accessing an operating system flag that indicates whether the requested file was changed prior to said close request;

computer code for scanning said requested file for computer viruses if said requested file was changed prior to said close request; and

computer code for skipping scanning said requested file if it was not changed prior to said close request.

10. The computer program product of claim 9, wherein said operating system flag is generated externally to said computer program product by the operating system in order to reduce redundant disk writes, whereby said computer code for scanning is invoked upon closing of the requested file only when actual disk writes are made by the operating system for the requested file.

A2

11. The computer program product of claim 10, wherein said computer code for accessing uses a file handle generated by the operating system to identify the operating system flag corresponding to the requested file, said handle having been generated when the file was opened.

12. A computer program product for detecting computer viruses on a file server, the file server providing file storage and retrieval services for at least one client computer over a network, said computer program product comprising:

computer code for detecting an open request from a client computer, the open request asking for a requested file from the file server;

computer code for scanning said requested file for computer viruses, whereby the file server is permitted to provide said requested file to the client computer if no computer viruses are found therein;

computer code for detecting a close request from the client computer associated with said requested file;

computer code for accessing an operating system flag that indicates whether the requested file was changed prior to said close request;

computer code for skipping scanning said requested file if it was not changed prior to said close request;

computer code responsive to said requested file having been changed prior to said close request for determining whether a virus vulnerable portion of said file was changed;

computer code for skipping scanning said requested file if a virus vulnerable portion of said file was not changed prior to said close request; and

computer code for scanning said requested file if a virus vulnerable portion of said file was changed prior to said close request.

13. The computer program product of claim 12, wherein said operating system flag is generated externally to said computer program product by the operating system in order to reduce redundant disk writes, whereby said computer code for scanning is invoked upon closing of the requested file only when actual disk writes are made by the operating system for the requested file.

14. The computer program product of claim 13, wherein said computer code for accessing uses a file handle generated by the operating system to identify the operating system flag corresponding to the requested file, said handle having been generated when the file was opened.